AFRL-AFOSR-VA-TR-2016-0184

Analysis and Algorithms for Imperfect Sensor Deployment and Operations

Joseph Guenes
UNIVERSITY OF FLORIDA

05/23/2016
Final Report

DISTRIBUTION A: Distribution approved for public release.

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ RTA2
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Service Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
20-05-2016	Final	01-08-2012 - 31-12-2015

4. TITLE AND SUBTITLE Analysis and Algorithms for Imperfect Sensor Deployment and Operations	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER FA9550-12-1-0353
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Jonathan Cole Smith	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) University of Florida Office of Engineering Research 339 Weil Hall Gainesville, FL 32611-6550	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AF OFFICE OF SCIENTIFIC RESEARCH 875 NORTH RANDOLPH STREET, RM 3112 ARLINGTON VA 22203	**10. SPONSOR/MONITOR'S ACRONYM(S)** AFOSR
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution A

13. SUPPLEMENTARY NOTES

None

14. ABSTRACT

The research begins by considering a class of problems in which a set of sensors has been deployed across some theater to monitor a set of targets, where sensors are subject to uncertain operation. In particular, it is usually appropriate to assume that a limited number of sensors can fail and erroneously report targets, or fail to detect targets that are indeed present. Simply using a redundant covering of targets is unnecessarily expensive, and thus more sophisticated methods are required to robustly cover a network in the presence of faulty sensors in a minimum-cost manner. This gives rise to the problem of minimizing the maximum number of "ambiguous nodes," i.e., nodes at which it is impossible to determine whether or not a target exists given the set of sensor readings. This core problem requires the invention of new network interdiction strategies, because the innermost recourse optimization problems in our scheme are integer programs, rather than linear programs (which can be dualized and solved as one monolithic integer programming problem). Therefore, this project explores applications and general theory that have clear benefit to the Air Force. This funding has created vital research opportunities for graduate students in the investigator's departments.

15. SUBJECT TERMS

Interdiction; Integer Programming; Optimization; Computation; Game Theory; Analytics

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			J. Cole Smith
U	U	U	UU	20	**19b. TELEPHONE NUMBER** *(Include area code)* 864-656-4716

Reset

DISTRIBUTION A: Distribution approved for public release.

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

Final Report: Analysis and Algorithms for Imperfect Sensor Deployment and Operations

AFOSR Grant FA9550-12-1-0353

PI: J. Cole Smith
Department of Industrial Engineering, Clemson University
(Initiated at the Department of Industrial and Systems Engineering, University of Florida)

Abstract

The research begins by considering a class of problems in which a set of sensors has been deployed across some theater to monitor a set of targets, where sensors are subject to uncertain operation. In particular, it is usually appropriate to assume that a limited number of sensors can fail and erroneously report targets, or fail to detect targets that are indeed present. Simply using a redundant covering of targets is unnecessarily expensive, and thus more sophisticated methods are required to robustly cover a network in the presence of faulty sensors in a minimum-cost manner. This gives rise to the problem of minimizing the maximum number of "ambiguous nodes," i.e., nodes at which it is impossible to determine whether or not a target exists given the set of sensor readings.

This core problem requires the invention of new network interdiction strategies, because the innermost recourse optimization problems in our scheme are integer programs, rather than linear programs (which can be dualized and solved as one monolithic integer programming problem). Therefore, this project explores applications and general theory that have clear benefit to the Air Force. We develop new techniques in interdiction problems, which have vast application to problems involving competition and strategy. This funding has created vital research opportunities for graduate students in the investigator's departments, and contributed to the core curriculum two universities in large-scale and discrete optimization.

1 Introduction

The economical and effective placement of sensors over a network is becoming a vital consideration for modern Air Force operations. One problem of considerable interest seeks to

DISTRIBUTION A: Distribution approved for public release.

strategically place sensors across a network so that a desired set of target locations is covered by at least one sensor. However, there are substantial risks that are undertaken when these sensors fail. In a battlefield scenario, a false positive reading from a sensor can impede a mission by causing undue delays while possible threats are investigated and ruled out. Worse, a false negative could fail to warn troops of impending attacks.

The problem that inspired the research in this proposal considered situations in which some sensors may incorrectly function by reporting false negatives or positives. In this case, the *status* of one or more nodes (i.e., whether or not a target is present at that node) can possibly be uncertain, depending on the set of sensor locations and the ones that fail to properly operate. (A failed sensor is capable of reporting false negatives and false positives at the locations it monitors.) The core problem that we consider assumes that there is a maximum number of sensors that can simultaneously fail when monitoring a network. If the status of a node is uncertain (i.e., it is impossible to tell whether or not a target exists at the node), we say that the node is ambiguous. Determining how vulnerable a sensor network is to attack requires one to (a) identify a set of nodes that can simultaneously fail, (b) compute a worst-case set of actual target locations, and (c) choose a set of faulty sensor readings, which collectively result in the maximum number of ambiguous nodes.

Although determining a sensor attack that maximizes the number of ambiguous nodes is quite difficult, it can be modeled as a compact integer linear programming problem. However, unlike contemporary research questions, we are posing a network interdiction model in which the inner problem (maximizing the number of ambiguous nodes) is not polynomially solvable. As a result, the now-standard method of dualizing the inner "attack" problem and combining it with the outer sensor location problem is not practical.

This difficulty requires us to investigate fundamentally new techniques for solving interdiction problems having NP-hard second-stage components. As a result, the research conducted by this grant led to genuine breakthroughs on how we approach the solution of *many* interdiction problems, whether or not the innermost problem is difficult. As we detail in this document, our methods have not only enabled the solution of interdiction problems when the inner stage is NP-hard, they have resulted in algorithms that are several orders of magnitude faster than the current state-of-the-art even when the inner stage is polynomially solvable.

The major goals of this proposal are given as below, with comments regarding the extent of our success following the original goals:

- *Examine special structures of the core min-max imperfect sensor location problem that can be exploited and solved within reasonable computational limits.*

DISTRIBUTION A: Distribution approved for public release.

  - This was achieved as planned, although the problems proved so difficult that only modest-sized instances could be solved within reasonable computational limits.

- *Abstract the interdiction techniques developed for the core problem, and generalize them to interdiction problems having two- (or multiple-) stage problems in which the second stage is NP-hard.*
  - This objective was achieved, and constitutes our biggest breakthrough.

- *Analyze complementary problems of interest to the Air Force involving stochastic target assessment problems, mobile target and dynamic sensor operations, and node deletion/monitoring problems on complex network structures.*
  - Work on node deletion and dynamic effects was recently completed. The basic foundations that would enable us to study dynamic problems, though, was not present and had to be developed in terms of shortest-path and assignment problems.

- *Integrate bilevel optimization research into courses at the University of Florida, with the goals of (a) illustrating contemporary optimization techniques and challenges to undergraduate students, and (b) encouraging Ph.D. students to work on security and defense problems that fall under the category of interdiction problems.*
  - This goal was achieved at Florida and at Clemson for graduate students. In particular, the PI offered a *Multilevel Mathematical Optimization* course in the Fall 2015 semester at Clemson. An elective offering that focuses on modeling will be offered at the undergraduate level at Clemson in Fall 2016.

The following section elaborates on the accomplishment of the first three goals, along with side projects that were successfully completed with AFOSR support.

2 Discussion of Research Accomplishments

The following papers describe the major findings of this research. All referenced papers refer to the PI's work in collaboration with his students and faculty colleagues.

DISTRIBUTION A: Distribution approved for public release.

2.1 Focused Sensor Application

We first give a complete description of the sensor problem described in Reference 18 by Sonuc and Smith. We consider sensor networks that attempt to monitor a collection of several critical locations in some environment in which various types of threats may exist. These threats may represent the physical presence of an entity in the environment (e.g., a fire or intruder), or some virtual entity such as a computer virus. These types of problems are often modeled by a network whose nodes represent locations that must be monitored by the network owner, and where an arc exists between two nodes if a sensor colocated at one node is able to determine whether there is an intruder at the other node. In this paper, the *status* of a node indicates whether or not a target exists at that node. The information sent from the sensors is collected as a set of *readings* at an administrative center, and made available to the network owner to assess the statuses of the nodes. However, due to the technical limits of the equipment used in the sensor systems (e.g., equipment failure, power shortage, equipment-specific capabilities) and also to the environmental factors that may degrade sensor function (e.g., hills, clouds, thunderstorms) the information received from the sensors may not always be accurate. The study of *fault-tolerant* sensor systems focuses on sensor networks in which a subset of deployed sensors might fail, and a faulty sensor might give a false positive or negative reading. In this paper, we study seven different cases on how the sensors might fail, and how the network owner utilizes knowledge of sensor functionality to assess where targets must or must not exist in the network.

We say that a node is *ambiguous* if and only if it is not possible to verify the status of that node with the current sensor readings. It is useful to envision an attacker that has somehow gained the ability to control the readings of any sensor that has failed, in order to maximize the number of ambiguous nodes. Hence, in this paper, we say that the attacker "hijacks" a set of sensors. Our class of problems can be represented as a *Stackelberg game* in which the attacker acts first by hijacking a limited number of the sensors on the network and manipulating their readings. The *defender* then ascertains, via the solution of a series of optimization problems, whether or not each node in the network is ambiguous. A critical consideration in determining node statuses is the maximum number of sensors that can simultaneously fail, which is a parameter, κ, that the defender utilizes to infer subsets of sensors that have failed. The role of interdiction here may actually represent an adversarial entity that seeks damage the sensor network, but could alternatively be viewed as a (worst-case) set of simultaneous sensor failures that could occur.

We model the relationship between the sensors and the nodes being monitored by a directed network $G = (N, A)$ with node set N and arc set A. An arc (u, v) belongs to A if and only

DISTRIBUTION A: Distribution approved for public release.

if a sensor at node u is capable of monitoring node v. We denote the index set of sensor locations by $S \subseteq N$, and of faulty sensors by $H \subseteq S$. Assume that a sensor can monitor itself, i.e., $(u, u) \in A$ if $u \in S$.

We assume that the maximum number of sensors that can simultaneously fail (κ) is known, which allows the defender to make inferences regarding which sensors have failed, and where targets must, or must not, necessarily exist in the network. Furthermore, the cases we study in this paper encompass four different options for the ability of the attacker to control the readings of hijacked sensors.

Option A The attacker possesses the ability to change the readings of all hijacked sensors to any value on any monitored node.

Option B A hijacked sensor always reports false readings on all nodes that it monitors.

Option C Each hijacked sensor reports at most one false reading.

Option D There exists an upper bound $\tau \geq 0$ on the total number of false readings on the network.

Additionally, the network owner may assume that the attacker only has certain capabilities. For instance, a problem classified as [A, C] means that the attacker can change all readings of all hijacked sensors, but the owner assumes that only one false reading per hijacked sensor could occur. Sonuc and Smith consider all pairs of assumptions in this regard.

Figure 1 illustrates how the node statuses are assessed when the defender assumes that the attacker can change all readings of each hijacked sensor (sensor 3 in this case) to any value. In Figure 1a, sensor 3 reports no target at node 3, and sensors 1 and 2 report a target at node 3. Since $\kappa = 1$, sensors 1 and 2 cannot be faulty at the same time, and so the defender knows that sensor 3 must be faulty. In this example, there is no accurate sensor monitoring node 5, which is therefore an ambiguous node. All other nodes are monitored by at least one accurate sensor (sensors 1 and 2). Given that the attacker aims to maximize the number of ambiguous nodes, it may report several correct readings in order to conceal the identity of faulty sensors. Figure 1b represents this action for sensor 3, where r_{33} is set to 1 in order to agree with sensors 1 and 2 on the status of node 3. In this case, both nodes 4 and 5 are ambiguous. (Note that r_{35} is irrelevant in both cases, and hence its value is omitted in Figures 1a and 1b.)

The foregoing examples show that the attacker does not wish to have hijacked sensors always report false readings (as it is optimal to have $r_{33} = 1$), or always report true readings (as

DISTRIBUTION A: Distribution approved for public release.

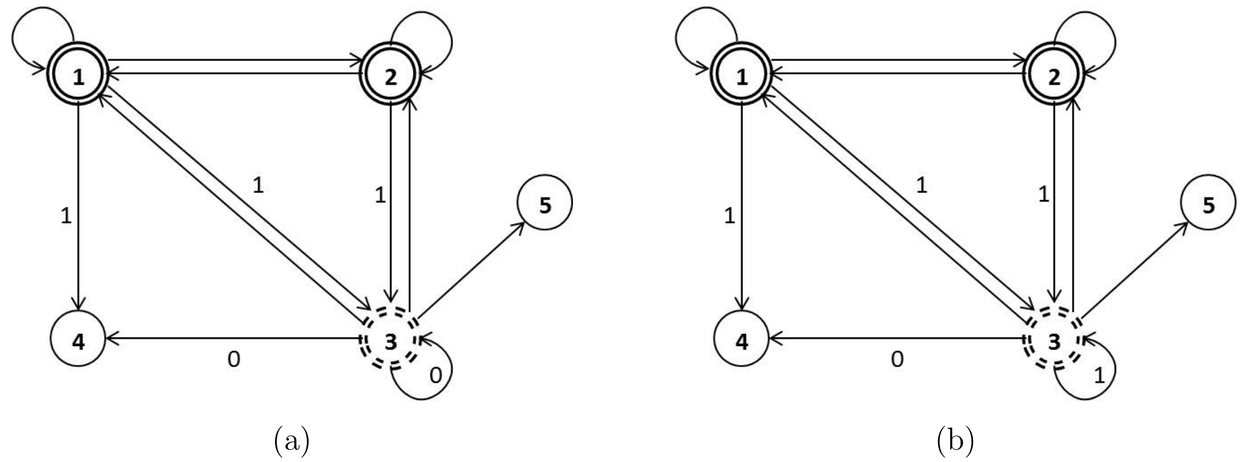


Figure 1: $S = \{1, 2, 3\}$, $H = \{3\}$, and $\kappa = 1$. **(a)** If $r_{33} = 0$, then node 5 is ambiguous. **(b)** If $r_{33} = 1$, then nodes 4 and 5 are ambiguous.

$r_{34} = 0$ is optimal). Furthermore, we observe that even when the defender ascertains which nodes belong to H, it is still possible for ambiguous nodes to exist (as is the case in Figure 1a). On the other hand, it is also possible to have no ambiguous nodes even if we cannot identify all faulty sensors (e.g., if G is a clique with $\kappa + 1$ nodes, sensors on all nodes, and $r_{ij} = 0$, $\forall i, j \in N$; however, this scenario corresponds to a suboptimal attacker action).

The methods for solving these problems by Sonuc and Smith all rely on single-level mixed-integer programming models. However, the scalability of those models is limited, which led to a more thorough investigation of theory and algorithms that underlie Stackelberg games, thus impacting our ability to solve network interdiction and robust optimization problems.

2.2 General Theory

2.2.1 Inner Convexification

Our first approach to tackling two-stage interdiction problems with integer variables in both stages was performed by Yen et al. (reference 11). In that paper, the first level player (*leader*) first determines its variables, which affect the second level player's (*follower*) optimization problem. With knowledge of the leader actions, the follower optimizes its objective, as per the traditional Stackelberg game. The authors study problems of the form

$$BP(\mathcal{W}, \mathcal{F}) : \qquad Z^*(\mathcal{W}, \mathcal{F}) = \min_{w \in \mathcal{W}} \max \{ p^\intercal x \mid (w, x) \in \mathcal{F} \},$$

DISTRIBUTION A: Distribution approved for public release.

where

$$\mathcal{W} = \mathcal{W}_R \cap \mathbb{Z}^m \text{ and } \mathcal{F} = \mathcal{F}_R \cap (\mathbb{Z}^m \times \mathbb{R}^{n-q} \times \mathbb{Z}^q)$$

with

$$\mathcal{W}_R = \{w \in \mathbb{R}^m \mid A_1 w \le b_1,\, 0 \le w \le u\},\ \mathcal{X}_R = \{x \in \mathbb{R}^n \mid A_2 x \le b_2,\, x \ge 0\},$$

and

$$\mathcal{F}_R = \left\{(w,x) \in \mathbb{R}^{m+n} \mid w \in \mathcal{W}_R,\, x \in \mathcal{X}_R,\, Cx + Dw \le d\right\}.$$

In the above definitions, A_1 is a rational $q_1 \times m$ matrix, while b_1 and u are rational q_1 and m-dimensional vectors, respectively. Further A_2, C, and D are rational $q_2 \times n$, $q_3 \times n$, and $q_3 \times m$ matrices. Finally, b_2, d, and p are rational q_2, q_3, and n-dimensional vectors, respectively. Most of the analysis in this work pertains to the case in which u is a general integer vector. However, our algorithmic developments are tailored to the situation in which variables w are binary, *i.e.,* $u = \mathbf{1}$ where $\mathbf{1}$ is a vector of suitable dimension whose entries are equal to 1.

The concept employed by this paper is to give a *restriction* of the follower's problem that can be solved via linear programming (as opposed to requiring the solution of an integer program). The advantage of this strategy is two-fold. One, we obtain a relaxation for the leader — the follower is restricted, after all — which gives a lower bound on the problem. Upper bounds can easily be obtained as well through this procedure. Two, finding a continuous restriction of the follower's problem then permits us to use standard dualization strategies for solving the resulting min-max optimization problem.

This algorithm is shown to be effective in solving integer knapsack and vertex cover interdiction problems, which is a new achievement in the literature. However, the worst-case behavior of this algorithm tends toward enumeration, and the scalability of the approach depends on special problem structures. These potential problems motivated a fundamentally different algorithm that does not explicitly rely on duality.

2.2.2 Sampling

Lozano and Smith (reference 12) consider a set of sampling-based algorithms for these problems. First, define $\mathbf{w}$, $\mathbf{x}$, and $\mathbf{y}$ as the decision variables for the first-, second-, and third-stage problems, respectively. We assume that the third-stage problem can take any general form, while the first- and second-stage problems include only binary variables, i.e., $\mathbf{w} \in \{0,1\}^{n_\mathbf{w}}$ and $\mathbf{x} \in \{0,1\}^{n_\mathbf{x}}$, where $n_\mathbf{w}$ ($n_\mathbf{x}$) is the number of variables required to model asset fortification (attack). Let $\mathcal{W}$ be the set of feasible solutions to the first-stage problem. Let $\mathcal{X}(\mathbf{w})$

DISTRIBUTION A: Distribution approved for public release.

be the set of feasible second-stage solutions given a defense vector $\mathbf{w}$, and let $\mathcal{Y}(\mathbf{x})$ be the set of feasible third-stage solutions for a given attack vector $\mathbf{x}$. Also, define $\mathcal{X} = \bigcup_{\mathbf{w} \in \mathcal{W}} \mathcal{X}(\mathbf{w})$ and $\mathcal{Y} = \bigcup_{\mathbf{x} \in \mathcal{X}} \mathcal{Y}(\mathbf{x})$, i.e., $\mathcal{X}$ and $\mathcal{Y}$ are the set of all possible second- and third-stage feasible solutions, respectively. Finally, let $f(\mathbf{y})$ be the defender's objective function.

We study problems of the form:

$$\mathcal{P}: \quad z^* = \min_{\mathbf{w} \in \mathcal{W}} \max_{\mathbf{x} \in \mathcal{X}(\mathbf{w})} \min_{\mathbf{y} \in \mathcal{Y}(\mathbf{x})} f(\mathbf{y}), \tag{1}$$

The first-, second-, and third-stage problems are known as *fortification*, *attack*, and *recourse* problems, respectively.

Reference 12 presents a novel backward sampling framework for solving three- (and two-) stage interdiction problems in which the recourse problem can take any form (e.g., it can be nonlinear, and can have integer variables), provided that all variables in the first two stages are restricted to be binary-valued. This framework is primarily designed to improve the solution of the interdiction problem, by solving relatively easy interdiction problem relaxations in which the defender is restricted to choose its recourse actions from a sample of the third-stage solution space. These problems provide upper bounds on the optimal interdiction solution; lower bounds can then be obtained by fixing an interdiction solution and optimizing the (original) recourse problem as a function of the fixed interdiction actions. This framework avoids linearizing a (potentially large) bilinear program, and also eliminates the need for applying combinatorial Benders' cuts at the interdiction stage (although we still require them to solve the fortification problem).

Using our framework, we were able to construct an algorithm for the shortest path interdiction problem with fortification. Our approach is far faster than the current state-of-the-art algorithm, finding optimal solutions over random grid networks having up to 3,600 nodes and 17,000 arcs, and over real-road networks having up to 300,000 nodes and more than 1,000,000 arcs. In particular, on some benchmark instances in the literature, our algorithms solved instances in an average of 95 seconds, where the current state-of-the-art algorithm (on the same computer) requires well over an hour on average and cannot solve certain instances within four hours. We also consider the capacitated lot sizing interdiction problem with fortification, in which the NP-hard third-stage problem is modeled as a MIP.

This same approach is used in a focused study on fortification-interdiction-routing games that take place over the traveling salesman problem (TSP) in reference 16. This study reveals that a straightforward implementation of the sampling approach in reference 12 is capable of solving three-stage games over the TSP, but a two-phase approach in which valid

DISTRIBUTION A: Distribution approved for public release.

inequalities are gleaned from approximate solutions to interdiction and routing problems substantially accelerates the solution process.

Lozano and Smith continue their approach in reference 13. For this problem, though, we consider problems in which the leader and follower play a two-stage game, but in which both agents play according to their own interests as opposed to a min-max or max-min setting. These so-called bilevel optimization problems are notoriously difficult, especially when integer restrictions govern the variables.

Formally, let $\mathbf{x}$ be an n_1-dimensional vector of integer variables controlled by the leader and $\mathbf{y}$ be an n_2-dimensional vector of variables controlled by the follower, where variables y_i, $i \in \mathcal{I} \subseteq \{1, \ldots, n_2\}$, are required to be integer-valued. Let $\phi^l(\mathbf{x}, \mathbf{y})$, $\phi^f(\mathbf{x}, \mathbf{y})$, $g_j^k(\mathbf{x})$, and $h_j^k(\mathbf{y})$ be continuous functions defined over $\mathbf{x}, \mathbf{y} \geq 0$, for $k = 1, 2$ and $j = 1, \ldots, m_k$. The bilevel mixed-integer program considered in reference 13 can be formally stated as:

$$z^* = \max_{\mathbf{x},\mathbf{y}} \ \phi^l(\mathbf{x}, \mathbf{y}) \tag{2a}$$

$$\text{s.t.} \ g_j^1(\mathbf{x}) + h_j^1(\mathbf{y}) \leq b_j^1 \qquad \forall j = 1, \ldots, m_1 \tag{2b}$$

$$\mathbf{y} \in \operatorname{argmax}\{\phi^f(\mathbf{x}, \mathbf{y}) \mid g_j^2(\mathbf{x}) + h_j^2(\mathbf{y}) \leq b_j^2, \ \forall j = 1, \ldots, m_2; \ \mathbf{y} \geq \mathbf{0}; \ y_i \in \mathbb{Z}, \ \forall i \in \mathcal{I}\} \tag{2c}$$

$$\mathbf{x} \in \mathbb{Z}_+^{n_1}, \tag{2d}$$

where $\mathbb{Z}_+^{n_1}$ denotes the set of all nonnegative integer vectors of dimension n_1. We assume that both the upper- and lower-level feasible regions are compact sets, and $g_j^2(\mathbf{x})$ is integer-valued for all $\mathbf{x} \in \mathbb{Z}_+^{n_1}$, $j = 1, \ldots, m_2$. (Note that if the lower-level problem has alternative optimal solutions, then the follower will select a $\hat{\mathbf{y}}$ that maximizes $\phi^l(\mathbf{x}, \mathbf{y})$, thus benefiting the leader. This is known as the *optimistic* formulation of the problem. We also consider a *pessimistic* formulation in the reference 13.)

The proposed algorithm in this paper also relies on establishing a partial enumeration of follower solutions. Unlike the case of interdiction problems, though, restricting the follower to select from a set of sampled solutions does not result in an upper bound on the leader's problem. Therefore, one of the primary challenges that Lozano and Smith address regards the development of lower- and upper-bounding mechanisms based on a sampling scheme for the follower. We contribute variable fixing and inequality generation schemes that accelerate the convergence of our algorithm, which we show runs up to 17 times faster than a current state-of-the-art approach for BMILPs over test instances from the literature. We also illustrate on a competitive scheduling problem why implicitly treating the objective as a nonlinear function is important in obtaining good computational results.

DISTRIBUTION A: Distribution approved for public release.

A parallel line of research was contributed by Buyuktahtakin et al. in reference 5. In fact, this paper does not study bilevel optimization problems at all, but is related due to the fact that it closely examines the optimal value function of problems that can be solved by dynamic programming (DP). In particular, some combinatorial problems can practically be solved by DP up to a certain number of states before the curse of dimensionality prohibits a complete execution of the algorithm due to memory limitations. However, our contribution in this paper is to show how a partial DP application can be used to glean tight inequalities that capture certain facets of the optimal value function to NP-hard problems. As such, they are related to value-function cuts employed in references 12 and 13.

2.2.3 Branch Decomposition

A third line of research is still ongoing at this time. One paper by Sonuc et al. has been completed, which seeks to capture solutions to difficult problems by using alternative network representations. Brambles and branch decompositions (see reference 9) comprise one avenue toward this goal. The concept is that certain NP-hard network problems can be solved by algorithms that are polynomial in terms of *branchwidth*. The branchwidth of a graph refers to the optimal objective function stemming from a mapping of a graph to a tree in which every node has degree 1 or 3. Hence, when branchwidth is small, solving problems that are NP-hard in general becomes practically very easy. In particular, the proposed algorithms that take place over the branch decomposition are based on dynamic programming, which can then possibly yield duality information, allowing us to solve stochastic integer programs (or interdiction, or robust optimization) using standard methods. The PI's student, Lozano, is working on expanding the research from reference 9 in this vein.

2.2.4 New Research Areas

The presence of dynamism in interdiction problems is novel and extremely challenging. Sefair and Smith propose two new problems and classes of algorithms to solve these problems.

For background, as discussed above, most contemporary network interdiction problems can be described as Stackelberg games in which two agents (a user and an attacker) with opposed interests interact in a network. In shortest-path interdiction (SPI), for instance, the user has the advantage of seeing the attacker's decisions before selecting its path. An alternative approach is taken in the robust shortest path (RSP) problem, in which the user first selects (and commits to) a path, and then the attacker interdicts arcs to maximally increase the

DISTRIBUTION A: Distribution approved for public release.

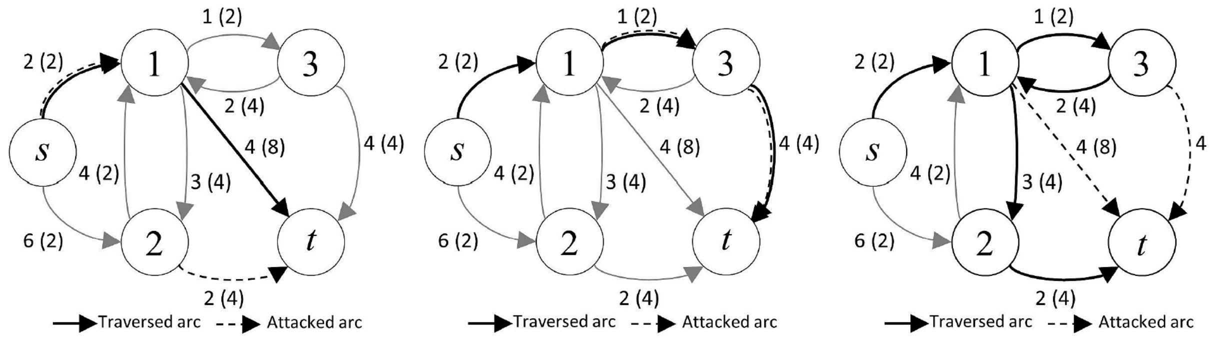
path's cost, given a budget constraint on the number of arcs that can be interdicted. In comparison to the SPI, the attacker is at an advantage in the RSP, having full knowledge of the user's path before taking any action.

To illustrate the interaction between the user and attacker, consider the graph depicted in Figure 2. Uninterdicted traversal costs are shown alongside each arc. If an arc is interdicted, its cost increases by the value shown in parentheses. (For instance, traversing arc $(1, t)$ has a cost of 4 if the arc is not interdicted, and a cost of 12 if it is interdicted.) Suppose that the user wants to move from node s to node t and that the attacker can interdict two arcs. Figure 2a illustrates the optimal SPI solution. In this case the optimal strategy for the attacker is to interdict arcs $(s, 1)$ and $(2, t)$. Given these attacks, the user follows the path $s \to 1 \to t$, which has an optimal cost of $z^*_{SPI} = 8$. Figure 2b illustrates the optimal solution for the RSP, in which the optimal user's path is $s \to 1 \to 3 \to t$. Given this path, the attacker interdicts arcs $(1, 3)$ and $(3, t)$, producing an optimal objective of $z^*_{RSP} = 13$. Not surprisingly, $z^*_{RSP} \geq z^*_{SPI}$, because the user has the advantage of knowing the interdicted arcs in the SPI, whereas the attacker has the advantage of knowing the user's path in the RSP.

Sefair and Smith (reference 14) propose algorithms for the *dynamic* shortest path interdiction (DSPI) problem, in which a cardinality-constrained attacker can interdict arcs whenever the user reaches a node in its path. The user sees all interdicted arcs, and is aware of the attacker's remaining budget. Accordingly, the user can adjust its path dynamically at any point in response to arc interdictions. Hence, the DSPI proceeds in multiple stages, where each stage consists of a (possibly empty) subset of arcs that are interdicted by the attacker, followed by an arc traversed by the user. These stages continue until the user reaches the destination node.

Figure 2c illustrates the DSPI. Initially, the attacker decides not to interdict any arc, and the user moves from s to 1. At this point, the attacker interdicts arc $(1, t)$, and the user moves from 1 to 3. Upon arrival at node 3, the attacker interdicts arc $(3, t)$ and the user decides to move back to 1. Because the attacker has no remaining budget, the user reaches the destination node by following the path $1 \to 2 \to t$. The optimal DSPI objective is thus given by $z^*_{DSPI} = 10$. This instance illustrates two insights into the nature of DSPI solutions. First, because the user knows the attacker's budget at all times, the user realizes upon visiting node 1 for the first time (and seeing the interdiction of $(1, t)$) that the attacker can interdict one more arc. Thus, using arc $(1, 2)$ at this point would induce the attacker to interdict arc $(2, t)$, trapping the user into traversing an expensive path to t. Second, note that unlike many other flow problems with nonnegative costs, it may be optimal for the user to return to previously visited nodes, as in this example.

DISTRIBUTION A: Distribution approved for public release.



(a) z^*_{SPI}=8 (b) z^*_{RSP}=13 (c) z^*_{DSPI}=10

Figure 2: Shortest-path interdiction, robust shortest path, and dynamic shortest-path interdiction

Sefair and Smith (reference 15) consider the Dynamic Assignment Interdiction (DAI) problem as well. In the DSPI, it is possible to solve the problem in polynomial time if the interdiction budget is small (i.e., there exist fixed-parameter tractable (FPT) models for DSPI). Interestingly, in the DAI, we prove that no FPT algorithm exists, because the DAI remains strongly NP-hard even when the attacker is limited to a single interdiction.

2.3 Applications

This subsection lists a brief summary of application-based work pursued based on the theoretical and methodological advances given above.

2.3.1 Containing Spread of Influence in Networks

In the study of Hemmati et al. (reference 4), we consider a network whose nodes can be influenced somehow by competing agents. These networks may model social or geographical interactions among entities, and influence can represent the spread of rumors, infections, or other types of transmissions over the nodes. A key question related to competition over such networks seeks to identify vital nodes in the network with the aim of protecting them from being the source of influence propagation from competing agents.

We consider a scenario in which two players, a defender and an attacker, compete on a directed network $G(V, A)$, where V is the set of nodes and A is the set of arcs. Initially,

DISTRIBUTION A: Distribution approved for public release.

the defender owns every node in the network, and can protect a subset of nodes against an impending action by the attacker. The attacker then acts, with full knowledge of the defender's action, to capture a set of unprotected nodes. For consistency with prior related studies, we say that captured nodes have been *influenced* by the attacker. This initial action takes place at time 0, and the game continues for T (discrete) time periods according to the following rules.

1. An influenced node remains influenced for the remainder of the time horizon.
2. A node that was protected by the defender cannot be influenced at any time.
3. Consider an unprotected node $j \in V$ that is not influenced at time $t \in \{0, \ldots, T-1\}$. Then node $j \in V$ becomes influenced at time $t+1$ if and only if there are some Q nodes $i \in V$ such that i is influenced at time t, and $(i, j) \in A$.
4. The attacker earns a reward of r_i^t if node i is influenced at time t (but not at time $t-1$, if $t \geq 1$).

The goal of the defender is to minimize the maximum sum of rewards that the attacker can earn (e.g., minimizing the maximum amount of damage that the attacker could possibly inflict on the defender's network). The algorithms employed rely on interdiction theory over time-expanded networks. A major contribution uses fast algorithms to analyze influence spread, and obtains dual information to a complex linear program without having to actually solve the linear program, which would be computationally inefficient.

2.3.2 Network Interdiction

Sullivan et al. in references 1 and 2 examine stochastic network interdiction problems, with reference 2 applying those studies to border security problems in the United States, and reference 1 studying the polyhedral aspects of these problems. In particular, reference 1 considers problems in which the evader and interdictor may have different perceptions of evasion probabilities. Sullivan and Smith, in Reference 6, also consider a fundamentally new problem in geometric network interdiction. (This paper appeared in *Networks* and won the Glover-Klingman prize for best paper in Networks for 2014.)

Sullivan and Smith consider the interdiction of a capacitated network that exists in Euclidean space. Nodes in this network exist at a point in space, and (directed) arcs connect node pairs in a straight line. An opponent wishes to maximize flow from a source node to a sink node

DISTRIBUTION A: Distribution approved for public release.

across the network, while an interdictor seeks to minimize the opponent's maximum flow by choosing multiple locations to attack. In this problem, attacks are made at points in (Euclidean) space. Damage is inflicted on each arc by reducing its capacity as a function of the distance from the midpoint of the arc to each attack. We refer to this problem as the *Euclidean maximum flow network interdiction problem* (E-MFNIP). While distance can be computed according to any norm, we focus on the case in which distances are computed by L_1-norms, which will enable us to derive mixed-integer linear programming formulations. Also, we assume that each arc capacity is a function of the distance from the center of the arc to the closest attack location. We provide mathematical programming-based approaches for solving E-MFNIP.

2.3.3 Robust Scheduling

Robust optimization is closely related to network interdiction, as described above for the Sefair and Smith papers. Tadayon and Smith consider robust scheduling problems in which a schedule is first derived, and then some data aspects (processing time, due dates, or other parameters) are determined after the fact. Unlike most papers in the field (see the Tadayon and Smith survey in reference 17), this study uses the more modern continuous "budgeted uncertainty" robust models. For instance, processing times may vary from their anticipated amounts, but the total processing time variation will be limited. Reference 7 explores a wide array of these problems, showing that some traditional scheduling principles still apply in the robustness case, while others immediately become invalid. Interestingly, even finding the worst-case set of processing times under the budgeted uncertainty model can become a very difficult problem, given a fixed schedule.

2.3.4 Competitive Set Covering Problems

The competitive set covering problem is a two-player Stackelberg (leader-follower) game involving a set of items and clauses. The leader acts first to select a set of items, and with knowledge of the leader's action, the follower then selects another subset of items. There exists a set of clauses, where each clause is a prioritized set of items. A clause is satisfied by the selected item having the highest priority, resulting in a reward for the player that introduced the highest-priority selected item. Like the bilevel problems explored by Lozano and Smith, the game here assumes that both players seek to maximize their profit, instead of working to reduce the other agent's profit.

DISTRIBUTION A: Distribution approved for public release.

Hemmati and Smith (reference 10) examine a bilevel mixed-integer programming formulation for a competitive set covering problem, which arises in non-cooperative product introduction and facility location games. Because binary decision variables appear in both stages of the model, this application fits under the proposed AFOSR research. Our contribution regards a cutting-plane algorithm, based on inequalities that support the convex hull of feasible solutions and are iteratively refined to induce faces in the largest dimension possible within practical computational limits.

2.4 Miscellaneous

Research conducted by the PI during this period that is not related to the proposed area is omitted from this report. However, there are two papers of interest to the AFOSR that have been conducted during this period, and are worth noting given their relevance to the AFOSR mission.

Multicommodity Flow Problems with Reliability Considerations. Tadayon and Smith (reference 3) consider a variation of the multicommodity flow (MCF) problem. The MCF typically seeks to satisfy demands among a set of commodities at minimum cost, across a directed network having capacitated arcs. The commodities are associated with an origin and destination node, and with a demand quantity. Additionally, many applications require flow between a commodity's origin and destination to follow a single path. Given flow costs for each arc on the network, the problem of simultaneously shipping all commodity demands on the network at a minimum cost where each commodity's flow follows a single path is referred to as the integer multicommodity flow problem.

Reference 3 examines integer MCFs on networks, in which intermediate nodes on an origin-destination path may fail to correctly deliver flows. For this problem, we assume that when a node fails to properly relay a commodity flow, the flow itself is propagated through the network as desired, but the contents of the flow have somehow been damaged. This may be the case in shipping fragile contents or in relaying information in a communication network. The reliability of each node (i.e., the probability that it correctly relays each commodity flow that passes through it) is modeled as a nonincreasing function of the load assigned to it, where load is given by the total amount of flow that crosses the node. Given an origin-destination route for each commodity, there exists a Boolean random variable corresponding to each commodity/node pair, which specifies whether or not the node will successfully relay the commodity flow. (For any node that does not serve as an intermediate node on the commodity's path, the random variable is irrelevant.) We assume that these random

DISTRIBUTION A: Distribution approved for public release.

variables are mutually independent, and so the probability of successfully transmitting flow on a path is calculated as the product of node reliabilities lying on the path.

The problem studied by Tadayon and Smith is the integer MCF, subject to the restriction that each commodity must be successfully delivered with a sufficiently large (specified) probability. We formulate the problem as a nonlinear multicommodity network flow problem, and prove that it is strongly NP-hard. We then present two linearization techniques for this formulation, and propose a pair of lower- and upper-bounding formulations, which can then be used within an exact cutting-plane algorithm to solve the problem.

Random Walk Reliability with Memory. Buke et al. in reference 8 consider a different type of reliability problem, which takes place over a network $G(V, A)$ having vertex set $V = \{1, \ldots, n\}$ and directed arc set A, where a reliability value $0 \leq r_{ij} \leq 1$ is associated with each arc $(i, j) \in A$. We examine some entity that conducts a random walk starting at node 1 (the origin node) and seeks to reach node n (the destination node). Define $\Delta_i = \{j \in V : (i, j) \in A\}$, and $\delta_i = |\Delta_i|$. Given that the entity is currently on node $i \in V$, the next arc traversed by the random walk is determined by selecting arc (i, j), where $j \in \Delta_i$, with probability $1/\delta_i$. We assume that there exists a directed path from node i to node n, for every $i \in V$.

The *survival probability* of a network is the probability that a random walk hits node n before it encounters an arc that fails while being traversed. In a truly Markovian model, the probability that an arc fails is independent of the walk's prior movements, and in fact a simple conditioning argument can be employed to compute the survival probability (as we show in Section 3). However, in several settings for which random walk analyses are conducted, an arc that is successfully traversed once is known to be reliable for the duration of the walk.

When an arc is known to be reliable after being successfully traversed once, we say that the arc has memory, or that it is a *memory arc*. A network may consist of a mixture of memory arcs and *memoryless arcs* (e.g., those arcs (i, j) that survive with probability r_{ij} each time they are traversed, independent of the number of times they have already been traversed).

The problem of calculating the survival probability is called the Random Walk Survivability problem with Memory (RWSM). Because of the arc memory property, simple Markov-chain methods are unsuitable for addressing the RWSM problem. In fact, there is no obvious way to compute a network's survival probability short of using an exponential-time algorithm. This paper makes three primary contributions. The first demonstrates that the RWSM is in general #P-hard, and in particular, is at least as hard as enumerating all Hamiltonian paths

DISTRIBUTION A: Distribution approved for public release.

in a directed network. The second provides two general approaches based on RWSM modifications, which (respectively) yield lower and upper bounds on the survival probability of a network. The third prescribes a mechanism for strategically constructing these modifications in order to produce tight bounds on survival probabilities.

3 Data on Accomplishments

The following is a list of papers submitted or accepted to refereed journals with AFOSR support. Note that papers 1–11 have been accepted (or appear), while the other papers are in various stages of review.

1. Sullivan, K.M., Smith, J.C., and Morton, D.P., Convex Hull Representation of the Deterministic Bipartite Network Interdiction Problem, *Mathematical Programming*, 145(1-2), 349-376, 2014.

2. Sullivan, K.M., Morton, D.P., Pan, F., and Smith, J.C., Securing a Border under Asymmetric Information, *Naval Research Logistics*, 61(2), 91-100, 2014.

3. Tadayon, B. and Smith, J.C., Algorithms for an Integer Multicommodity Network Flow Problem with Node Reliability Considerations, *Journal of Optimization Theory and Applications*, 161(2), 506-532, 2014.

4. Hemmati, M., Smith, J.C., and Thai, M.T., A Cutting-plane Algorithm for Solving a Weighted Influence Interdiction Problem, *Computational Optimization and Applications*, 57(1), 71-104, 2014.

5. Buyuktahtakin, I.E., Smith, J.C., Hartman, J.C., and Luo, S., Parallel Asset Replacement Problem under Economies of Scale with Multiple Challengers, *The Engineering Economist*, 59(4), 237-258, 2014.

6. Sullivan, K.M. and Smith, J.C., Exact Algorithms for Solving a Euclidean Maximum Flow Network Interdiction Problem, *Networks*, 64(2), 109-124, 2014.

7. Tadayon, B. and Smith, J.C., Algorithms and Complexity Analysis for Robust Single-Machine Scheduling Problems, *Journal of Scheduling*, 18(6), 575–592, 2015.

8. Buke, B., Smith, J.C., and Thomas, S.A., On a Random Walk Reliability Problem with Arc Memory, *Networks*, 66(1), 67–86, 2015.

DISTRIBUTION A: Distribution approved for public release.

9. Sonuc, S.B., Smith, J.C., and Hicks, I.V., A Branch-and-Price-and-Cut Method for Computing an Optimal Bramble, *Discrete Optimization*, 18, 166–188, 2015.
10. Hemmati, M. and Smith, J.C., A Mixed-Integer Bilevel Programming Approach for a Competitive Prioritized Set Covering Problem, *Discrete Optimization*, to appear.
11. Yen, J., Richard, J.-P., and Smith, J.C., A Class of Algorithms for Mixed-Integer Bilevel Min-Max Optimization, *Journal of Global Optimization*, to appear.
12. Lozano, L. and Smith, J.C., A Backward Sampling Framework for Interdiction Problems with Fortification, minor revision submitted to *INFORMS Journal on Computing*.
13. Lozano, L. and Smith, J.C., A Sampling-Based Exact Approach for the Bilevel Mixed Integer Programming Problem, under revision for *Operations Research*.
14. Sefair, J. and Smith, J.C., Dynamic Shortest-Path Interdiction, submitted to *Networks*.
15. Sefair, J. and Smith, J.C., Exact Algorithms and Bounds for the Dynamic Assignment Interdiction Problem, submitted to *SIAM Journal on Optimization*.
16. Lozano, L., Smith, J.C., and Kurz, M.E., Solving the Traveling Salesman Problem with Interdiction and Fortification, submitted to *Operations Research Letters*.

These publications are also peer-reviewed, and appear in edited books or encyclopedias.

17. Tadayon, B. and Smith, J.C., A Survey of Robust Offline Single-Machine Scheduling Problems, *Wiley Encyclopedia of Operations Research and Management Science* (edited by J. Cochran), Wiley, Hoboken, NJ, 2015.
18. Sonuc, S. and Smith, J.C., Models for Assessing Vulnerability in Imperfect Sensor Networks, In: *Dynamics of Information Systems: Algorithmic Approaches* (edited by A. Sorokin, M. Banghart, P.M. Pardalos, and R. Murphey), 2013.

Also, the PI received the Glover-Klingman Prize for best paper in *Networks* in 2014.

The following Ph.D. students have received their degrees during this period, with the support of the AFOSR.

1. Mehdi (Soheil) Hemmati, Multilevel Discrete Formulations and Algorithms with Applications to New Product Introduction Games and Network Interdiction Problems, August 2013.

DISTRIBUTION A: Distribution approved for public release.

2. Andrew Romich, Mixed-Integer Nonlinear Algorithms and Analysis for Spatial Network Interdiction Problems, August 2013. Co-advised with Dr. Guanghui Lan.

3. Yen Thi-Ha Tang, A Class of Algorithms for Mixed-Integer Bilevel Min-Max Optimization Problems with Applications, December 2013. Co-advised with Dr. J.-P. Richard.

4. Bita Tadayon, Algorithms and Complexity Analysis for Integer Multicommodity Network Flow and Robust Single-Machine Scheduling Problems, May 2014. [

5. Shantih Spanton, Network Models for Performance Analysis and Optimization, August 2014. Co-advised with Dr. Joseph Geunes.

6. Sadie Thomas, Survival Probability on Networks with Memory and Fortification, December 2014.

7. Jorge Sefair, Interdiction Models for Planning Under Uncertainty, August 2015.

Current Ph.D. students Leonardo Lozano-Sanchez and Robert M. Curry have worked on portions of this research. Their anticipated graduation dates are August 2017 and August 2018, respectively.

The PI has given the following presentations on AFOSR-related research during the reporting period. These are in addition to those seminars given by the Ph.D. students supported by this grant.

1. "A Robust Sensor Covering and Communication Problem," Invited Lecture, Industrial and Systems Engineering Research Conference, May 2013, San Juan, PR.

2. "Revisiting Fortification Algorithms for Facility Interdiction Problems," Invited Lecture, University of Buffalo, February 2014, Buffalo, NY.

3. "Revisiting Fortification Algorithms for Facility Interdiction Problems," Invited Lecture, University of Southern California, March 2014, Los Angeles, CA.

4. "Revisiting Fortification Algorithms for Facility Interdiction Problems," Invited Lecture, University of Tennessee, March 2014, Knoxville, TN.

5. "Dynamic Shortest Path Interdiction," Invited Lecture, 2015 INFORMS Computing Society Conference, Virginia Commonwealth University, January 2015, Richmond, VA.

6. "A Backward Sampling Framework for Interdiction Problems with Fortification," Invited Lecture, Bogazici University, May 2015, Istanbul, Turkey.

DISTRIBUTION A: Distribution approved for public release.

7. "A Backward Sampling Framework for Interdiction Problems with Fortification," Invited Lecture, Sabanci University, May 2015, Istanbul, Turkey.

8. "A Backward Sampling Framework for Interdiction Problems with Fortification," Invited Lecture, Koc University, May 2015, Istanbul, Turkey.

9. "Dynamic Shortest Path Interdiction," Invited Lecture, The Ohio State University, August 2015, Columbus, OH.

10. "Dynamic Shortest Path Interdiction," Invited Lecture, Florida State University, September 2015, Tallahassee, FL.

11. "Dynamic Shortest Path Interdiction," Invited Lecture, Northwestern University, October 2015, Chicago, IL.

12. "Dynamic Shortest Path Interdiction," Invited Lecture, University of Minnesota, October 2015, Minneapolis, MN.

13. "A Backward Sampling Framework for Interdiction Problems with Fortification," Invited Lecture, Universidad de los Andes, October 2015. Bogota, Colombia.

14. "Concepts in Integer Programming, Interdiction, and Robust Optimization," Invited Lecture, Tsinghua University, November 2015. Beijing, China.

DISTRIBUTION A: Distribution approved for public release.

1.

1. Report Type

Final Report

Primary Contact E-mail
Contact email if there is a problem with the report.

jcsmith@clemson.edu

Primary Contact Phone Number
Contact phone number if there is a problem with the report

864-656-4716

Organization / Institution name

Clemson University

Grant/Contract Title
The full title of the funded effort.

Analysis and Algorithms for Imperfect Sensor Deployment and Operations

Grant/Contract Number
AFOSR assigned control number. It must begin with "FA9550" or "F49620" or "FA2386".

FA9550-12-1-0353

Principal Investigator Name
The full name of the principal investigator on the grant or contract.

Jonathan Cole Smith

Program Manager
The AFOSR Program Manager currently assigned to the award

Fariba Fahroo

Reporting Period Start Date

08/01/2012

Reporting Period End Date

12/31/2015

Abstract

The research begins by considering a class of problems in which a set of sensors has been deployed across some theater to monitor a set of targets, where sensors are subject to uncertain operation. In particular, it is usually appropriate to assume that a limited number of sensors can fail and erroneously report targets, or fail to detect targets that are indeed present. Simply using a redundant covering of targets is unnecessarily expensive, and thus more sophisticated methods are required to robustly cover a network in the presence of faulty sensors in a minimum-cost manner. This gives rise to the problem of minimizing the maximum number of "ambiguous nodes," i.e., nodes at which it is impossible to determine whether or not a target exists given the set of sensor readings.

This core problem requires the invention of new network interdiction strategies, because the innermost recourse optimization problems in our scheme are integer programs, rather than linear programs (which can be dualized and solved as one monolithic integer programming problem). Therefore, this project explores applications and general theory that have clear benefit to the Air Force. We develop new techniques in interdiction problems, which have vast application to problems involving competition and strategy. Applications include network interdiction and fortification, mitigating the spread of influence throughout networks, and bilevel programming problems. Further, the research contributed here

incorporate dynamic interdiction problems for the first time. This funding has created vital research opportunities for graduate students in the investigator's departments, and contributed to the core curriculum two universities in large-scale and discrete optimization.

Distribution Statement

This is block 12 on the SF298 form.

Distribution A - Approved for Public Release

Explanation for Distribution Statement

If this is not approved for public release, please provide a short explanation. E.g., contains proprietary information.

SF298 Form

Please attach your SF298 form. A blank SF298 can be found here. Please do not password protect or secure the PDF The maximum file size for an SF298 is 50MB.

Form 298 Smith.pdf

Upload the Report Document. File must be a PDF. Please do not password protect or secure the PDF . The maximum file size for the Report Document is 50MB.

FA9550_12_1_0353_Final_Report.pdf

Upload a Report Document, if any. The maximum file size for the Report Document is 50MB.

Archival Publications (published) during reporting period:

Sullivan, K.M., Smith, J.C., and Morton, D.P., Convex Hull Representation of the Deterministic Bipartite Network Interdiction Problem, Mathematical Programming, 145(1-2), 349-376, 2014.

Sullivan, K.M., Morton, D.P., Pan, F., and Smith, J.C., Securing a Border under Asymmetric Information, Naval Research Logistics, 61(2), 91-100, 2014.

Tadayon, B. and Smith, J.C., Algorithms for an Integer Multicommodity Network Flow Problem with Node Reliability Considerations, Journal of Optimization Theory and Applications, 161(2), 506-532, 2014.

Hemmati, M., Smith, J.C., and Thai, M.T., A Cutting-plane Algorithm for Solving a Weighted Influence Interdiction Problem, Computational Optimization and Applications, 57(1), 71-104, 2014.

Buyuktahtakin, I.E., Smith, J.C., Hartman, J.C., and Luo, S., Parallel Asset Replacement Problem under Economies of Scale with Multiple Challengers, The Engineering Economist, 59(4), 237-258, 2014.

Sullivan, K.M. and Smith, J.C., Exact Algorithms for Solving a Euclidean Maximum Flow Network Interdiction Problem, Networks, 64(2), 109-124, 2014.

Tadayon, B. and Smith, J.C., Algorithms and Complexity Analysis for Robust Single-Machine Scheduling Problems, Journal of Scheduling, 18(6), 575-592, 2015.

Buke, B., Smith, J.C., and Thomas, S.A., On a Random Walk Reliability Problem with Arc Memory, Networks, 66(1), 67-86, 2015.

Sonuc, S.B., Smith, J.C., and Hicks, I.V., A Branch-and-Price-and-Cut Method for Computing an Optimal Bramble, Discrete Optimization, 18, 166-188, 2015.

Hemmati, M. and Smith, J.C., A Mixed-Integer Bilevel Programming Approach for a Competitive Prioritized Set Covering Problem, Discrete Optimization, to appear.

Yen, J., Richard, J.-P., and Smith, J.C., A Class of Algorithms for Mixed-Integer Bilevel Min-Max Optimization, Journal of Global Optimization, to appear.

Lozano, L. and Smith, J.C., A Backward Sampling Framework for Interdiction Problems with Fortification, minor revision submitted to INFORMS Journal on Computing.

Lozano, L. and Smith, J.C., A Sampling-Based Exact Approach for the Bilevel Mixed Integer Programming Problem, under revision for Operations Research.

Sefair, J. and Smith, J.C., Dynamic Shortest-Path Interdiction, submitted to Networks.

Sefair, J. and Smith, J.C., Exact Algorithms and Bounds for the Dynamic Assignment Interdiction Problem, submitted to SIAM Journal on Optimization.

Lozano, L., Smith, J.C., and Kurz, M.E., Solving the Traveling Salesman Problem with Interdiction and Fortification, submitted to Operations Research Letters.

Tadayon, B. and Smith, J.C., A Survey of Robust Offline Single-Machine Scheduling Problems, Wiley Encyclopedia of Operations Research and Management Science (edited by J. Cochran), Wiley, Hoboken, NJ, 2015.

Sonuc, S. and Smith, J.C., Models for Assessing Vulnerability in Imperfect Sensor Networks, In: Dynamics of Information Systems: Algorithmic Approaches (edited by A. Sorokin, M. Banghart, P.M. Pardalos, and R. Murphey), 2013.

Changes in research objectives (if any):

N/A

Change in AFOSR Program Manager, if any:

N/A

Extensions granted or milestones slipped, if any:

A one-year extension was granted to the PI at Clemson University. Hence, this report is "final" in the sense that it

AFOSR LRIR Number

LRIR Title

Reporting Period

Laboratory Task Manager

Program Officer

Research Objectives

Technical Summary

Funding Summary by Cost Category (by FY, $K)

	Starting FY	FY+1	FY+2
Salary			
Equipment/Facilities			
Supplies			
Total			

Report Document

Report Document - Text Analysis

Report Document - Text Analysis

Appendix Documents

2. Thank You

E-mail user

May 20, 2016 23:39:40 Success: Email Sent to: jcsmith@clemson.edu